What is Claimed Is:

1.   1.   A digital file forming a contract comprising:

2.   a header package having rules defining sealed packages produced by a

3. sealing party;

4.   a body containing at least a portion of the content of the contract; and

5. a validating signature generated from said rules and said body according to a first key

6. belonging to a validating party; and

7.   a sealing signature generated from said header package and said sealed

8. packages according to a second key belonging to said sealing party.

1.   2.   A digital file forming a contract according to claim 1 wherein said header

2. package further comprises a unique header identifying a type of said sealed package and

3. wherein said validating signature is generated from said rules, said body and said header.

1.   3.   A digital file forming a contract according to claim 1 wherein said sealed

2. package comprises a unique number generated by said sealing party and said sealing

3. signature is generated from said header package, any of said sealed packages and said

4. unique number.

1.   4.   A digital file according to claim 1 wherein said rules define one or more

2. unsealed packages to be included in said sealed package, said body comprises a HTML

3. file and one of the unsealed packages defined in the rules contains data for a field in the

4. HTML file.

1.   5.   A digital file according to claim 1 wherein said rules comprise a URL

2. corresponding to the location for which each sealed package to be included in the contract

3   can be obtained.

1   6.   A digital contract according to claim 5 wherein said URL is a CGI script

2   for commanding a remote server to generate said sealed package.

1   7.   A digital contract according to claim 5 wherein said URL identifies the

2   location of said sealed package.

1   8.   A contract management apparatus for validating a digital file constituting a

2   contract, said digital file having a header package which includes rules defining sealed

3   packages, a body containing at least a portion of the contract, and a validating signature,

4   comprising:

5   means for reading said rules and for identifying a validating party and a

6   sealing party which created a sealed file of said contract;

7   first means for obtaining a first key belonging to said validating party

8   cooperable with said validating signature generated from said rules and body to validate

9   said header package;

10   second means for obtaining a second key belonging to said sealing party

11   cooperable with said sealing signature to validate said contract; and

12   means for iteratively validating any sealed packages contained in said

13   contract using said second key and sealing signature.

1   9.   A contract management apparatus as claimed in claim 8 wherein said

2   iterative validating means returns any data stored in said sealed packages.

1   10.   The contract management apparatus of claim 9 further comprising means

2   for displaying said body contents and said returned data.

1   11.   A contract management apparatus for generating a digital file constituting

2   a contract comprising:

3   means for obtaining a header package for said contract;

4   means for reading rules defining sealed data packages, and for identifying

5   a sealing party and any sealed packages to be included in said contract;

6   means for obtaining said identified sealed packages;

7   means for generating a sealing signature from said header package and any

8   of said sealed packages according to a first key belonging to said sealing party; and

9   means for assembling said header package, sealed packages and said

10   sealing signature into said digital file constituting a contract.

1   12.   A contract management apparatus comprising:

2   means for accepting and securely storing data files constituting contracts in

3   an encrypted package database;

4   means for backing-up said package database;

5   a navigator tool adapted to allow a user access to said stored data files

6   constituting said contracts;

7   means, responsive to a request for an encrypted package from said data

8   base, for transmitting said package to an external entity;

9   means for informing users of data files having expiring contracts in said

10   data base; and

11   means for deleting contracts from said data base.

1   13.   The contract management apparatus of claim 8, including one of a

2   smartcard, a personal digital assistant, a personal computer, a terminal or an embedded

3   system.

1   14.   A computer product for storing instructions which are executed by a

2   computer to validate a digital file having a header package which includes rules defining

3   sealed packages, a body containing at least a portion of a contract and a validating

4   signature, comprising:

5   reading said digital file and identifying a validating party and a sealing

6   party which created a sealed package of said contract;

7   deriving a first key belonging to a validating party;

8   validating said header package using said first key and said validating

9   signature;

10   deriving a second key belonging to said sealing party;

11   deriving a sealing signature from said header package; and

12   validating said digital file using said second key and said sealing signature.

1   15.   The computer product according to claim 14, further comprising

2   instructions for deriving said sealing signature from a unique number contained in said

3   header package.

1   16.   A computer product storing instructions for execution on a computer to

2   perform a process to validate a digital file constituting a contract comprising the steps of:

3   unzipping a header package in said digital file and reading rules contained

4   in said header package;

5   determining from said rules keys to validate said header package and a

6   sealed package of said digital file constituting said contract; and

7   validating each sealed package in said digital file using said keys.

1   17.   The computer product storing instructions for execution on a computer

2   according to claim 16, further comprising instructions for performing the additional steps

3   of obtaining said keys from a network server identified by said rules.

1   18.   A computer product for storing instructions for a computer to execute the

2   process comprising the steps of:

3   storing rules to describe a data package;

4   creating from said rules a data package containing a digital data file;

5   merging said rules and said data package into a merged file;

6   creating a package validity signature from said merged file to prevent

7   unauthorized use of said digital file; and

8   generating a unique number identifying said digital file;

9   merging said package validity signature, said merged file and said unique

10   number;

11   creating a sealing signature from said merged files; and

12   sealing said merged files with said sealing signature to produce a sealed

13   package.

1   19.   A computer product according to claim 18 wherein said rules comprises a

2   plurality of elements which point to a location on said computer containing a required

3.   package.

1   20.   The computer product according to claim 19 wherein said rules define a

2   sealing signature for said sealed package.

1   21.   The computer product according to claim 18 wherein said merged files are

2   compressed as a single file.